INTRODUCTION (1)

Welcome to the Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) Overview module, designed to familiarize you with the new common PIV identification standard for federal employees and contractors.

GOALS (2)

The goal of this training module is to increase your awareness of HSPD-12 and the corresponding technical standard FIPS 201.

HSPD-12 is a policy that establishes a common standard for a secure and reliable form of identification for federal employees and contractors.

FIPS 201 defines a government-wide Personal Identity Verification (PIV) system, where common identification badges can be created and used to verify a person's identity. This module will discuss how the new requirements affect federal agencies deploying the badge.

HSPD-12 (3)

Homeland Security Presidential Directive 12 (HSPD-12) establishes a common standard for a secure and reliable form of identification for federal employees and contractors. HSPD-12 compliant identification is:

- Issued based on sound criteria for verifying an individual employee's identity.
- Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation.
- Rapidly authenticated electronically.
- Issued only by providers whose reliability has been established by an official accreditation process.

IMPORTANCE OF HSPD-12 (4)

In 2004, the President determined that the current identity badges used for physical access to federal facilities vary widely. Therefore, there is often no trust or reciprocity between federal agencies.

HSPD-12 improves interoperability between federal agencies by requiring them to adopt stronger security standards and procedures, providing a consistent method for issuing identity badges, and addressing access to facilities and information technology (IT) systems and applications.

BENEFITS OF HSPD-12 (5)

HSPD-12 establishes the concept of "one process, one badge". A common badge will improve security throughout the federal government by providing a common method of validating an identity for level of access to facilities and information technology systems using a consistent and reliable issuance process built upon a chain of trust.

FIPS 201 (6)

The FIPS 201 standard was created by the National Institute of Standards & Technology (NIST), and is the implementation directive for HSPD-12. It defines a government-wide PIV controls and requirements system. In this system, a common process for issuing badges based on identity vetting through a certified chain of trust, is implemented in all federal agencies, allowing use of the badges to verify an individual's identity. It is important to understand that this process does not address permission to access government resources, such as computer systems and physical locations.

IMPORTANCE OF FIPS 201 (7)

FIPS 201 is an important standard because it establishes consistent, repeatable processes to ensure personnel are accurately identified. It provides for a uniform badge that can be recognized and electronically processed within and between federal agencies. FIPS 201 improves authentication by relying on centralized systems and management processes to create reliable identification badges and interoperable information exchange capabilities.

FIPS 201 AND PRIVACY (8)

FIPS 201 maintains personal privacy by adhering to federal privacy laws and policies. Data stored on the Badge is encrypted, with additional protection provided by a Personal Identification Number (PIN) chosen by the recipient. The PIN can only be accessed by a card reader. This makes it extremely difficult to duplicate or forge. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks.

The digital biometric data are encrypted in the card. The data are locked into the card by the issuing authority and cannot be modified by anyone other than the issuing authority. Social Security Numbers are not kept on the card. Instead, each person will have a unique identifier called a Uniform Universal Personal Identification Code (UUPIC) that is used in place of Social Security Numbers. The UUPIC is randomly generated and is not a variant of the person's Social Security Number; therefore, the Social Security Number cannot be derived from the UUPIC.

PIV & THE CHAIN OF TRUST (9)

PIV defines the requirements for issuing a trusted identity badge that is recognized as valid outside the agency from which it was issued. PIV includes policies and procedures for identity proofing and registration, ensuring that sufficient information is provided by the Applicant to reliably establish their identity. This assurance is termed the "Chain of Trust".

A chain of trust is the linkage of steps in a secure system starting with validation of the identity of the individual requesting a badge. A secure PIV system provides the federal government with confidence in the authentication of the person's identity credentials, in

the identity token issuing organizations, and other components of the automated system. The chain of trust must also ensure that information entered into and used within the system is verified, protected and used appropriately. The steps in NIH's chain of trust are:

- Adopt and use an identity proofing and registration process that meets the FIPS 201 requirements.
- Require the applicant to appear in person at least twice. Once with two forms of identity source documents in original form, and the second time when the badge is issued to the applicant.
- Complete an FBI fingerprint check on the applicant.
- Initiate, at a minimum, a National Agency Check with Written Inquiries.
- Check the biometrics of the applicant at issuance.
- Ensure that no single individual can issue a badge.

BADGES (10)

PIV defines the technical standards for the badge to electronically authenticate personnel. The badge must contain embedded chips. The chips will be discussed in more detail later in this presentation. Agencies must have the ability to load the required data and authentication certificates onto the badge. PIV defines a common framework for how the badge can provide basic interoperability across the federal government.

FEATURES OF BADGES (11)

The new badges are similar in size to NIH's current badges. The chips can store various forms of data that help identify the cardholder and how long the badge can be used before it expires. Data stored on the chips will include: information to identify the card, identity certificates, electronic keys that can be used for encryption, a Federal Agency Smart Credential Number (FASC-N), and fingerprint minutiae. This data is used to verify a cardholder's identity in order to grant access to a facility or information system.

TYPES OF BADGES (12)

NIH federal employees and personnel under contract to and visiting NIH, to include foreign nationals (which includes Lawful Permanent Residents (LPR)) working for NIH, use two common badges to access NIH facilities and information technology systems. The common badges are:

- HHS PIV Card - for NIH employees, contractors and affiliates who will need regular or long term access to NIH facilities or information systems
- NIH ID Badge - for NIH employees, contractors and affiliates who will need temporary or intermittent access to NIH facilities or information systems

What Roles are Required for PIV (13)

FIPS 201 identifies roles in the PIV process. NIH uses the following terminology for these roles:

- The Applicant is the individual who needs to access NIH resources, such as systems or facilities. This includes employees, contractors, and affiliates.
- The Sponsor provides initial data about the Applicant and submits a PIV request on behalf of the Applicant.
- The Sponsor validates the relationship between the Applicant and the agency.
- The Registrar initiates a background investigation, if necessary, or verifies that current background investigations meet NIH's minimum requirements.
- The Registrar is the authorizing official for the issuance of a badge to an Applicant who has met all proofing, enrollment, and investigative requirements.
- The Registrar validates Applicant's identity and captures identity information and biometrics.
- The Issuer validates Applicant's identity; encodes, finalizes, and issues the badge to the Applicant; and collects and destroys the Applicant's prior badge when applicable.

These roles, performed by trusted individuals, are vital to the chain of trust. If you are assigned to perform one of the roles in the PIV workflow, it is essential that you execute your duties as specified in NIH's policies and procedures. This will ensure that the chain remains intact and that the badges NIH issues can be trusted by all government agencies.

PIV WORKFLOW (14)

This is a high-level overview of how an Applicant obtains a badge.

1. The request is initiated and sponsored.
2. The Applicant appears before the Registrar and supplies documentation proving his identity, as well as biometric data (photograph and fingerprints), and is enrolled into the PIV system.
3. The necessary background checks are performed and the request is authorized.
4. The badge is issued.

Next, we will show what PIV roles interact with each step in the PIV Workflow.

BADGE REQUEST (15)

During the Requesting process:

The Applicant provides basic demographic data to the Sponsor. The Applicant is the individual who needs routine physical access to NIH facilities or information technology (IT) systems. This includes employees, contractors, and affiliates.

The Sponsor performs initial entry of the Applicant's demographic data into the system as part of the badge request.

The Sponsor validates the relationship between the Applicant and the agency. A Sponsor may not also perform the roles of Registrar or Issuer.

IDENTITY PROOFING AND ENROLLMENT (16)

During the Identity Proofing and Enrollment process:

The Applicant appears in person and presents two forms of identity source documents that are listed on Form I-9 (OMB No. 1615-0047, Employment Eligibility Verification) for validation; poses for pictures; and provides fingerprints.

The Registrar captures the Applicant's fingerprints, biometric information, and photo. The fingerprints are used for the background investigation and for encoding fingerprint minutiae onto the badge. The Registrar also scans and validates the I-9 documents, ensuring agreement between the Applicant's name and information appearing on the I-9 documentation, as well the information previously entered into the PIV system by the Sponsor. Finally, the Registrar determines whether the Applicant's reasons for any I-9 discrepancies discovered during proofing, such as the use of a different name, are valid and acceptable.

INVESTIGATION (17)

During the Investigation process:

The Applicant completes the investigation forms or electronic questionnaire.

The Registrar reviews the sponsorship and results of I-9 validation and investigations, and records the final results.

The Registrar adjudicates the results of the prior investigations and determines what type of enrollment the Applicant needs to complete. The Registrar cannot fill any other role in the PIV process.

The Federal Office of Personnel Management (OPM) carries out background investigations.

The FBI performs fingerprint checks, providing the results back to the agency and OPM.

BADGE ISSUANCE (18)

During the Issuance process:

The Registrar authorizes the production and issuance of a badge.

The Applicant presents their current badge for revocation, provides fingerprints for validation, provides an I-9 document for identity validation, selects a PIN for encoding onto the badge, and accepts custodial responsibility for the new badge.

The Issuer verifies that the I-9 document presented by the applicant is valid, encodes the badge, and checks the biometrics that were previously recorded during enrollment to verify that the same individual is present for issuance. The Issuer collects and destroys the old badge, and issues a new badge. In addition, the Issuer manages the encoding and inventory of cards (badges).

PIV PROCESS SUMMARY (19)

You have seen how the PIV process and the issuance of badges support HSPD-12. If you have been assigned a role in the PIV Process, you will take additional training that is specific to your role.

ADDITIONAL INFORMATION (20)

This ends the PIV Overview Training module. If you need more information on the PIV Workflow or your role in it, you can visit the HSPD-12 website (IDBadge.nih.gov); view the PIV Training module specific to your role; review FIPS 201; or contact the NIH HSPD-12 Program Office at 301-496-3067.